

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-355272

(43) 公開日 平成11年(1999)12月24日

(51) Int.Cl.<sup>6</sup>

H 0 4 L 12/22  
12/56

識別記号

F I

H 0 4 L 11/26  
11/20

1 0 2 A

審査請求 未請求 請求項の数14 O L (全 19 頁)

(21) 出願番号 特願平11-126563

(22) 出願日 平成11年(1999) 5月 7日

(31) 優先権主張番号 0 9 / 0 7 4 7 4 5

(32) 優先日 1998年 5月 8日

(33) 優先権主張国 米国 (U S)

(71) 出願人 596092698

ルーセント テクノロジーズ インコーポ  
レーテッド

アメリカ合衆国, 07974-0636 ニュージ  
ャーシー, マレイ ヒル, マウンテン ア  
ヴェニュー 600

(72) 発明者 ムーイ チョー チュー

アメリカ合衆国 07724 ニュージャーク  
シー, イートンタウン, イートンクレスト  
ドライブ 148ビー

(74) 代理人 弁理士 岡部 正夫 (外11名)

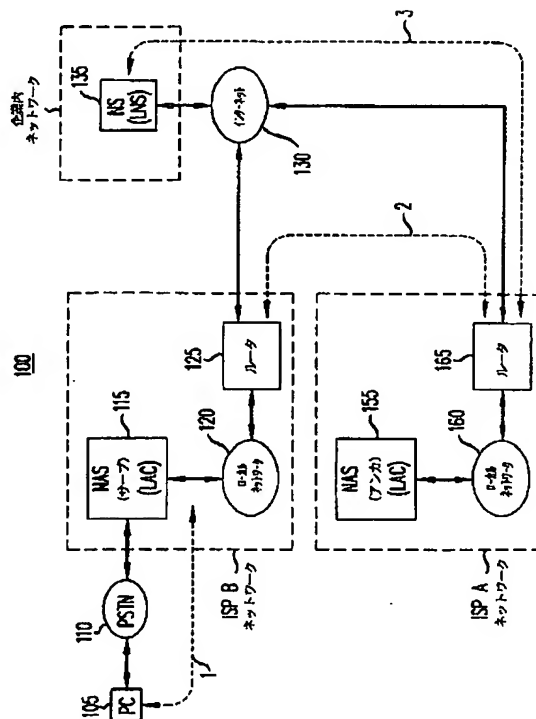
最終頁に続く

(54) 【発明の名称】 多重ホップ・ポイント・ツー・ポイント・プロトコル

(57) 【要約】

【課題】 本発明は、通信におけるパケット通信システムに関し、特に多重トンネルによる私設網への遠隔アクセスを可能にする仮想私設網 (V P N) サービスに関する技術を提供する。

【解決手段】 本発明は、パケット・サーバで使用される方法であって、他のパケット終端間に多重ホップ・パケット・トンネルを確立する段階と、該多重ホップ・パケット・トンネルを通じて該他のパケット終端間でメッセージを中継する段階とからなることを特徴とする。これにより、多数のインターネット・サービス・プロバイダ (I S P) を通じて仮想ダイヤルアップ・サービスが提供され、特に、遠隔ユーザはサブ I S P への接続を確立することによって仮想ダイヤルアップ・サービスにアクセスする。サブ I S P は、アンカ I S P への第 1 トンネルを確立する。アンカ I S P は、例えば、私設イントラネットへのトンネルを確立する。その結果、多重トンネルによる私設網への遠隔アクセスを可能にする仮想私設網 (V P N) サービスが提供される。



**【特許請求の範囲】**

【請求項 1】 パケット・サーバで使用される方法であって、該方法が、他のパケット終端間に多重ホップ・パケット・トンネルを確立する段階と、該多重ホップ・パケット・トンネルを通じて該他のパケット終端間でメッセージを中継する段階とからなることを特徴とする方法。

【請求項 2】 請求項 1 に記載の方法において、該確立する段階が、1 つのパケット終端への第 1 のパケット・トンネルを確立する段階と、別のパケット終端への第 2 のパケット・トンネルを確立する段階とからなることを特徴とする方法。

【請求項 3】 請求項 2 に記載の方法において、該方法はさらに、接続情報を追跡する段階からなり、該接続情報は、該第 1 のパケット・トンネルに関するトンネル識別値と該第 2 のパケット・トンネルに関するトンネル識別値とを含む段階を含むことを特徴とする方法。

【請求項 4】 請求項 1 に記載の方法において、該中継段階は、該他のパケット終端間で中継する前に該メッセージの少なくとも一部を修正する段階を含むことを特徴とする方法。

【請求項 5】 請求項 1 に記載の方法において、該中継段階は、該他のパケット終端間で中継する前に該メッセージの少なくとも一部のトンネル識別情報を修正する段階を含むことを特徴とする方法。

【請求項 6】 請求項 1 に記載の方法において、該中継段階は、該他のパケット終端間でメッセージを中継する前に、該パケット・サーバに関するパケット処理遅延を含む何れかのメッセージに含まれるパケット処理遅延情報を修正する段階を含むことを特徴とする方法。

【請求項 7】 請求項 1 に記載の方法において、該パケット・サーバが多重トンネルをサポートするインターネット・プロトコルを使用することを特徴とする方法。

【請求項 8】 請求項 7 に記載の方法において、該インターネット・プロトコルがレイヤ 2 トンネル・プロトコルの形態であることを特徴とする方法。

【請求項 9】 パケット・ネットワークで使用される装置であって、該装置が、

a) 仮想私設網サービスにアクセスするためにユーザとのポイント・ツー・ポイント・プロトコル接続を承認し、そして b) ホップ間に配置されホップ間でメッセージを中継するように、他のパケット・サーバとの多重ホップ・トンネル接続を承認するパケット・サーバからなることを特徴とする装置。

【請求項 10】 請求項 9 に記載の装置において、該パケット・サーバは、該メッセージの少なくとも一部をホップ間で中継する前に修正することを特徴とする装置。

【請求項 11】 請求項 9 に記載の装置において、該パ

ケット・サーバは、該メッセージの少なくとも一部のトンネル識別情報をホップ間で中継する前に修正することを特徴とする装置。

【請求項 12】 請求項 9 に記載の装置において、該パケット・サーバは、ホップ間でメッセージを中継する前に、該パケット・サーバに関するパケット処理遅延を含む何れかの該メッセージに含まれるパケット処理遅延情報を修正することを特徴とする装置。

【請求項 13】 請求項 9 に記載の装置において、該パケット・サーバは、多重トンネルをサポートするインターネット・プロトコルを使用することを特徴とする装置。

【請求項 14】 請求項 13 に記載の装置において、該インターネット・プロトコルがレイヤ 2 トンネル・プロトコルの形態であることを特徴とする装置。

**【発明の詳細な説明】****【0001】**

【発明の属する技術分野】本発明は、概して、通信に関し、特にパケット通信システムに関する。尚、関連する主題が、本出願と同じ日付で出願された「移動ポイント・ツー・ポイント・プロトコル」という名称の特許出願で開示されている。

【0002】通信手段としてのインターネットの用途の 1 つは、ワークグループを互いに結合していわゆる「仮想私設網」(Virtual Private Network: VPN)を提供する高度データ・バックボーンとしての使用法である。VPN の応用例の 1 つは、従業員が、例えば、自宅でインターネットを通じて企業のデータ・ネットワークに遠隔アクセスできる企業環境におけるものである。VPN は、公衆設備を使用するにもかかわらず、閉じたユーザ・グループに参加する遠隔ユーザにセキュリティと認証を提供する。事実上、VPN を使用することによって、企業とその従業員には WAN と同様の手段が提供される(ユーザが直接企業のネットワークにダイヤルする等の方法で、企業のネットワークが直接遠隔アクセスを提供することもできるが、VPN を使用の方が経済的に有利である。)

【0003】VPN を提供するために、「ポイント・ツー・ポイント・トンネル・プロトコル」(Point-to-Point Tunneling Protocol: PPTP)や「レイヤ 2 フォワーディング」(Layer 2 Forwarding)プロトコルといったトンネル・プロトコルが使用される。一般的に言って、トンネル・プロトコルは、1 つのパケットを別のパケットの内部に配置することにより、公衆網を通じて専用データ・ストリームを作成することを可能にする。VPN の場合、IP パケットが別の IP パケットの内部に配置される。業界標準の開発を目指して、インターネット・エンジニアリング・タスク・フォース(Internet Engineering Task Force: IETF)は、「レイヤ 2 トンネル・プロトコル」(Layer 2 Tunneling

Protocol: L2TP)を開発しているが、これはPPTPとL2Fプロトコルの混成物である(例えば、K.Hamzeh、T.Kolar、M.Littlewood、G.Singh Pall、J.Taard、A.J.Valencia及びW.Vertheinの「レイヤ2トンネルプロトコル」L2TP”(Layer Two Tunneling Protocol “L2TP”)(Internet draft、1998年3月)を参照されたい。))。

【0004】遠隔ユーザにとって、VPNにアクセスする通常の形態は、「在来型の電話サービス」(Plain-Old-Telephone Service: POTS)接続により、VPNを提供する「インターネット・サービス・プロバイダ」(Internet Service Provider: ISP)にアクセスすることである。例えば、ユーザは、アナログモデムをパーソナル・コンピュータまたはその相当品に組み込み、特定ISP(ここでは「ホーム」ISPと呼ぶ)のカスタマ・アカウントを取得する(ユーザのパーソナル・コンピュータが上記のトンネル・プロトコルの1つをサポートするよう正しく設定されていることも前提となる)。ユーザは、「ホーム」ISPに関連する電話番号をダイヤルするなどして簡単にホームISPにデータ呼出を行った後VPNに「ログイン(logging in)」してVPNにアクセスする。

#### 【0005】

【発明の概要】上記で説明したトンネル・プロトコルによっては、遠隔ユーザはVPNにアクセスする際、ホームISP以外のISPにはログインできないことが認識された。今日の移動通信の領域において、特にユーザが呼の継続中に物理的位置を変えるパーソナル・コミュニケーション・サービス(Personal Communication Service: PCS)無線環境の場合、これは大きな制約である。言い換えれば、遠隔ユーザが位置を変える際、ホームISPは、少なくとも一時的にはユーザに利用できなくなり、ユーザのVPNへのアクセスは阻止される。

【0006】従って、本発明によれば、パケット・サーバは他のパケット終端間に多重ホップ・トンネルを確立し、多重ホップ・トンネルの部分間でメッセージを中継する。すなわち、遠隔ユーザは、ホームISPに加えて訪問中のISPによるVPNへのアクセスが可能になる。

【0007】本発明の実施例によれば、多数のインターネット・サービス・プロバイダ(ISP)を通じて仮想ダイヤルアップ・サービスが提供される。特に、遠隔ユーザは、サーバISP(serving ISP)への接続を確立することによって仮想ダイヤルアップ・サービスにアクセスする。サーバISPは、アンカISPへの第1トンネルを確立する。アンカISPは、例えば、私設イントラネットへのトンネルを確立する。その結果、多重トンネルによる私設網への遠隔アクセスを可能にする仮想私設網(Virtual Private Network: VPN)サービスが提供される。

#### 【0008】

【発明の詳細な記述】すでに言及したように、本出願は、上記のChuah他の特許出願に関連している。すなわち、詳細な説明は参照を容易にするため3つの節に分けられる。

【0009】<多重ホップ・ポイント・ツー・ポイント・プロトコル>図1は、本発明の原理による例示としての通信システム100を示す。本発明の概念以外、構成要素は周知であるので、詳細には説明しない。例えば、パーソナル・コンピュータ(Personal Computer: PC)110には、公衆電話網(Public-Switched-Telephone Network: PSTN)110を通じてISP Bにダイヤルアップ接続し、インターネット接続を確立するデータ通信機器(図示せず)が含まれる。同様に、通信システム100の構成要素間の実線は対応する終端間の周知の通信機能を表している。例えば、PC110とPSTN110間の接続は加入者回線接続を表し、ISP Bとインターネット120間の接続は同期光通信網(Synchronous Optical Network: SONET)を通じて非同期転送モード(Asynchronous Transfer Mode: ATM)によってサポートされる等である。さらに、読者は上記のL2TPプロトコルに精通していることが前提になる。

【0010】図1から見られるように、通信システム100は、ISP Aネットワークによって表されるISP Aと、ISP Bネットワークによって表されるISP Bの2つのISPを備えている。ISP Bネットワークは、当業技術分野で周知の接続点(Point-Of-Presence: POP)ルータを含むネットワーク・アクセス・サーバ(Network Access Service: NAS)115、ローカル・ネットワーク120およびルータ125を備えている。同様に、ISP Aネットワークは、NAS155、ローカル・ネットワーク160およびルータ165を備えている。ISP Aが、例示としての企業のネットワークにネットワーク・サーバ(Network Server: NS)135を通じてアクセスする遠隔地に位置する従業員にVPNサービスを提供することが想定されているが、このNS135は多くの機能の中でも特に、ルーティングとファイアウォール機能を提供する(企業のネットワークは、例えば、NS135の背後で適切に保護されたローカルエリア・ネットワーク(図示せず)の集合であると想定される)。

【0011】遠隔ユーザが、一時的にせよ、国内の、ISP AのサービスではなくISP Bのサービスの対象になる部分に位置することがあるのが観察された。さらに、ISP AがそのVPN対象範囲を他の範囲に拡大しようとすることがある。従って、本発明の原理によれば、遠隔ユーザは自分のホームまたはアンカISPに加えて訪問中またはサーバISPを通じてVPNにアクセスすることができる(ISP AとISP Bが別のサ

ービス・プロバイダであることが想定されるが、これは必ずしも本発明の概念ではない。例えば、同じISPの中の別個のネットワークであってもよい。すなわち、PC105に位置するユーザ（図示せず）は、国内を、例えば、移動しながら企業のネットワークにアクセスすることができる。

【0012】この時点で、次の定義が前提となる。

mL2TP— K.Hamzeh, T.Kolar, M.Littlewood, G.Singh Pall, J.Taarud, A.J.Valencia及びW.Vertheinの「レイヤ2トンネルプロトコル”L2TP” (LayerTwo Tunneling Protocol ”L2TP”)」(Internet Draft, 1998年3月) およびここで説明される修正によって定義されるL2TPプロトコル。

LAC— mL2TPアクセス制御装置、すなわち、mL2TPをサポートするNAS。

LNS— mL2TPをサポートするNS。

アンカLAC— VPNサービスを提供するLNSへのトンネルをサポートするLAC。

サブLAC— アンカLACへのトンネルをサポートするLAC。

(これらの定義は本発明の概念の例示としての説明を単純化するために使用される。すなわち、当業者が認識するように、本発明の概念はこのように制限されるものではなく、あらゆるトンネル・プロトコルと関連処理機器に適用できる。)

【0013】本発明の概念によれば、ISP AネットワークはアンカLAC115を示し、ISP BネットワークはサブLAC115を示す。以下さらに説明されるように、本発明の原理によれば、図1の通信システム100は多重ホップ・トンネルを提供する。図1の例は、2つのホップ・トンネルを示す。1つのホップはISP BネットワークからISP Aネットワークに至り、もう1つのホップはISP Aネットワークから企業のネットワークに至っている。

【0014】ここで図2を参照すると、本発明の原理による方法の高レベル流れ図が示される(サブLAC115と他のそれぞれのサーバは、従来のプログラミング技術を使用して以下に説明する方法を実行するよう適切にプログラムされていると考えられるが、ここで使用されるプログラミング技術は周知のもので説明しない)。ステップ205では、遠隔ユーザがPSTN110を通じてISP BへのPPP(ポイント・ツー・ポイント・プロトコル)接続を開始する。ステップ210では、サブLAC115が(例えば、所定の「ユーザ名」または「パスワード」を使用して)部分的にユーザを認証し、(図1の点線1で表される)接続を承認する(また、DNIS(Dialed Number Identification Service:ダイヤル番号識別サービス)、CLID(Calling Line Identification:発呼回線識別)または他の同等の形態の識別法が使用されることもある)。

明らかに、サブLAC115がユーザを認証できない場合、接続は承認されない(このステップは図示されていない)。

【0015】(背景として、また当業技術分野で周知のように、遠隔ユーザが新しいPPPセッションの開始を希望する場合、PC110はサブLACに対してPPPLCP(Link Control Protocol:リンク制御プロトコル)構成要求(ConfigRequest)を開始する。本発明の概念によれば、サブLACは、アンカLACとの通信を開始する前に、ユーザの機器と、当業技術分野で周知のように、PPPLCPとPPP PAP/CHAP両方の段階を完了する。(安全なコンジットのために、IETFは、パスワード認証プロトコル(Password Authentication Protocol:PAP)とチャレンジャーハンドシェイク認証プロトコル(Challenge-Handshake Authentication Protocol:CHAP)という、PPP接続のセキュリティのための2つのプロトコルを定義した(例えば、IETF Request for Comment(RFC)1334、「PPP認証プロトコル」を参照されたい。))

【0016】ステップ215では、サブLAC115が、遠隔ユーザがVPNサービスの使用を希望していると判断する(この選択は、特定の「ユーザ名」に直接関連し、および/または、例えば、サービスLAC115が提供するポップアップ「ハイパーテキスト・トランスポート・プロトコル(Hyper Text Transfer Protocol:HTTP)フォームによるなどの、ユーザからの個別の要求に関連する)。遠隔ユーザが仮想ダイヤルアップ・サービスを要求しない場合、サブLAC115はステップ220で標準インターネット・アクセスを提供する。しかし、遠隔ユーザがVPNの使用を希望する場合、サブLAC115はステップ225で関連するアンカLACを特定する(以下説明する)。

【0017】サブLAC115は、例えば、ユーザのIDを特定のアンカLACにアプライオリに関連づけるVPNテーブルを保存している。こうしたテーブルの一部を以下表1に示す。この例では、PC110に関連する遠隔ユーザが、アンカLACであるISPA.com、すなわちアンカLAC115に関連している。

【表1】

ユーザID	アンカーLAC
ユーザ名	ISPA.com

表1

【0018】(単に「ユーザ名@ISPA.com」といった形で構成されたフィールドのリストを維持するといった同等の構造または操作が使用されることもあることに留意されたい。なお、ここでは@記号の後の部分はアンカLACを示す。また、ISP Bがユーザをサービスにマップするデータベースを維持することもある。仮想ダイヤルアップ、すなわち、遠隔ユーザをVPNサ

ービスに関連するものとして特定する場合、このマッピングはさらにアンカLACを特定する。また、当業技術分野で周知のように、サブLACはこのタスクのためにローカルラディアスサーバ(local radius server)とのラディアスアクセス要求/応答トランザクションを使用することもある)

【0019】ステップ230では、サブLAC115が、サブLAC115自体とアンカLAC155の間

にトンネルがあるかを確認する。すなわち、サブLAC115は、トンネル識別(Tunnel identification: Tid)値、現在そのトンネルを使用する呼の関連呼識別子(Call identifiers: Cid)および関連するアンカLACのIPアドレスによって表される現行トンネルの、以下表2で示されるようなテーブルを保守する。

【表2】

Tid	Cid	アンカLAC IPアドレス
2	5	h. j. k. l

表2

【0020】サブLACとアンカLACの間にトンネル接続が現在存在しない場合、ステップ235で、サブLAC115によってアンカLACへのトンネルが確立される(以下説明する)。サブLACとアンカLACの間にトンネルが存在する場合、サブLAC115は、ステップ240で、新しいCidを割り当て、表2を更新し、(以下さらに説明するように)ローカル・ネットワーク120、ルータ125、インターネット130、ルータ165およびローカル・ネットワーク160を通じてVPN要求をアンカLAC155に転送する。この要求の中で、サブLAC115はユーザ識別情報をアンカLAC155に伝える。

【0021】ここで図3を参照すると、アンカLAC155はステップ305で要求を受信する。ステップ310では、アンカLAC155はさらに(例えば、上記で言及した所定の「ユーザ名」と「パスワード」を使用して)遠隔ユーザの認証を行い、(図1の点線2で表される)接続を承認する(また、サブLACと同様、DNIS、CLIDまたは他の同等の形態の識別が使用されることもある)。アンカLAC155がユーザを認証できない場合、接続は承認されない(このステップは図示されていない。この場合、サブLAC115は同様にエラーメッセージを遠隔ユーザ(図示せず)に返送しなければならない。)

【0022】アンカLAC155は、例えば、ユーザの

接続番号	サブLAC		LNS	LNS	ユーザに割り当てられたIPアドレス
	Tid	Cid	Tid	Cid	
5	2	5	1	3	a. b. c. d

表4

【0025】アンカLACは、接続番号を各VPNセッションに関連づける。さらに、この接続番号は対応するユーザにマップ(map)される。この表は、接続番号によって、(そのホップの関連トンネルIDと呼ID値を伴う)サブLACのIPアドレスと、(その関連するホップの関連トンネルIDと呼ID値を伴う)関連LNSのIPアドレスを列挙する。ステップ330では、アン

IDを特定のLNSにアプライオリに関連づけるVPNテーブルを保存している。こうしたテーブルの一部を以下表3に示す。この例では、PC110に関連する遠隔ユーザが、IPアドレスg. h. i. jによって表されるLNS135に関連している。

【表3】

ユーザID	LNS
ユーザ名	g. h. i. j

表3

【0023】(サブLAC115と同様に、同等の構成または動作が使用できることに留意されたい。例えば、アンカLACは、ホームラディアスサーバ(Home Radius Server)により、ラディアスアクセス要求/応答メッセージを通じてこの機能を行うことがある。)ステップ315では、アンカLAC155は、表3を使用してこれが有効な要求かを確認する。これが有効な要求でない場合、アンカLAC155はステップ320で要求を拒否する。これが有効な要求である場合、アンカLACはステップ325で表3から関連LNSを識別する。

【0024】アンカLACは、遠隔ユーザとの間に確立された各VPNセッションについて、各通信方向に関する次の接続テーブルを保守していると想定される。

【表4】

カLAC155がVPNセッションを確立する(認証の確認等を行う)。(ここでも、LNS135が(例えば、遠隔ユーザの認証ができない場合や遠隔ユーザを受け入れる余地がないために)VPN要求を拒否した場合、アンカLACとサブLACによって適当なエラーメッセージが生成される)。本発明の概念以外に、LNS135とのVPNセッションが当業技術分野で周知の

ように確立される。例えば、本発明の原理によれば、新しいVPNセッションを確立する際に、アンカLAC155は新しいCidを割り当て、表4を更新する（例えば、新しい接続を割り当てる）。この最後の接続は、図1の点線3によって表される。

【0026】この時点で、連結性はポイント・ツー・ポイントPPPセッションであり、その終端は、一方では（PC110によって表される）遠隔ユーザのネットワーク・アプリケーションであり、もう一方ではこの連結性のLNS135PPPサポートへの終端である（必要な場合、LNSと共にサブLAC、アンカLACで課金処理を行えることに留意されたい。すなわち、各構成要素はパケット、オクテット、接続の開始・終了時間をカウントすることができる）。

【0027】上記の多重ホップ仮想ダイヤルアップ・サービスをサポートする目的で、ある形式のL2TP（mL2TP）プロトコルが使用されるが、これについて以下説明する。L2TPでは、各LAC-LNSペア間の制御メッセージと、同じLAC-LNSペア間のパイロード・パケットという所定のトンネルで動作するmL2TPの2つの並列コンポーネントが存在する。後者は、LAC-LNSペア間のユーザ・セッションに関するmL2TPカプセル化PPPパケットを転送する。L2TPでは、Nr（次の受信）およびNs（次の送信）フィールドが常に制御メッセージに表示され、必要に応じてパイロード・パケットに存在する。制御メッセージとパイロード・メッセージは別のシーケンス番号状態を使用する。上記のLAC/LNSペアのシナリオでは、（Nr、Ns）の保守と使用に関する限りL2TPドラフト・プロトコル定義の変更はない。

【0028】しかし、サブLACとアンカLACの間の接続では、アンカLACはサブLACが送信する（Nr、Ns）値を監視するだけである。すなわち、本発明の概念によれば、アンカLACは単純にサブLACから受信した値をLNSに再送信する。さらに、アンカLACはここで、サブLACが送信したパケットから観察された対応する（Nr、Ns）値によって（受信状態、送信状態）値（Sr、Ss）を更新する。サブLACとアンカLACの間には疑いなくパケット損失が存在するので、アンカLACのSs（Sr）値はサブLACのSs（Sr）値より小さい（小さい）。さらに、アンカLACは、サブLAC/アンカLAC制御接続に関するものと、アンカLAC/LNS制御接続に関するものとの2組の（Sr、Ss）変数を保守する。

【0029】PPPトンネルが形成される前に、本発明の概念によれば、サブLAC、アンカLACおよびLNSの間で制御メッセージを交換しなければならない。制御メッセージは、後にmL2TP制御管理情報が伝えられた場合パイロード・データの転送に使用されると同じトンネルを通じて交換される（後で説明する）。

【0030】本発明の概念によれば、追加属性値ペア（additional Attribute Value Pairs:additional AVP）（後で説明する）が定義され、L2TP制御メッセージ（ひいてはmL2TP制御メッセージとなる）で使用される。この追加AVPは上記で説明した多重ホップ機能と呼転送機能をサポートするためのものである。L2TPの定義では、AVPはさらに制御信号を指定するためにも使用される。

【0031】上記で言及したように、上記で説明したLAC/LNSペアの場合、上記で言及したL2TPドラフトで説明した手順に変更はない。すなわち、以下説明する追加手順が必要になるのは、多重ホップの場合だけである。

【0032】多重ホップ・メッセージの流れの例を図4に示す。図4から観察されるように、サブLACとアンカLACの間にトンネル（Tid値で示される）と呼（Cid値で示される）が確立される。同様に、アンカLACとLNSの間にトンネルと呼が確立される。図4に示すように、本発明の概念はサブLACがアンカLACへのトンネルを確立することを要求する。本発明では、サブLACはアンカLACをLNSとして扱い、L2TP手順が使用されてトンネルを初期設定する。

【0033】トンネルが確立されると、多数の制御メッセージ・トランザクションが発生し、本発明の原理によってPPPセッションを設定する。それらは図5-図7に示される。これらの図では、様々な制御メッセージの関連フィールドだけが図示される（サブLACとアンカLAC間のトンネルのトンネルidおよび呼idが、アンカLACとLNS間のそれらの数値と異なっている場合、アンカLACはそれらを何れかの方向に中継する前にパケット・ヘッダの関連フィールドを修正する）。

【0034】図5に示すように、サブLACはまず開始制御接続要求（Start-Control-Connect-Request Message(SCCRQ)）メッセージ（L2TPの定義による）をアンカLACに送信し、両者間にトンネルを設定する。このメッセージを受信すると、アンカLACは開始制御接続一応答（Start-control-Connect-Reply Message(SCCRP)）によって応答する（これは上記で説明した何らかの認証に続いて行われる）。サブLACは開始制御接続一接続（Start-Control-Connection-Connect(SCCCN)）メッセージによってアンカLACに対する確認を行う。

【0035】図5に示す開始制御接続（Start-Control-Connection）メッセージの交換に続いて、サブLACは、図6に示すように、着信呼要求（Incoming-Call-Request(ICRQ)）メッセージをアンカLACに送信する。着信呼要求（Incoming-Call-Request）メッセージにはアンカLACがLNSを識別するのに十分なユーザ・データと信用証明が含まれている。

【0036】前に述べたように、アンカLACとLNSの間にトンネルが存在しない場合、アンカLACは、L

2 T P の定義により、L N S との S C C R、S C C R P、S C C C N メッセージ交換を開始する。トンネルが存在する場合、トンネル内の未使用スロットである C i d がアンカ L A C によって割り当てられる。この時点で、本発明の原理によれば、アンカ L A C は I C R Q メッセージを（サブ L A C から）中継し、L N S にこの新しいダイヤルアップ・セッションについて通知する。図 6 に示すように、アンカ L A C は I C R Q メッセージを L N S に中継する前にしかるべく修正する。修正されたフィールド、例えば、割当て呼 I D は、“\*”によって示される。アンカ L A C はまた隠し A V P を追加し、L N S にサポート可能な受信ウィンドウ・サイズを知らせる（追加ホップの場合、アンカ L A C は制御／ペイロード両方の接続について取り決められた最大ウィンドウ・サイズを記録することに留意されたい。また、サブ L A C とアンカ L A C 間の制御接続のウィンドウ・サイズがアンカ L A C と L N S 間の制御接続のものと異なっており、バッファリングが必要なことがある。バッファリングとシーケンス番号監視の追加を避けるために、アンカ L A C は必要に応じて、アンカ L A C がアンカ L A C からサブ L A C の方向でサポートできるペイロード・セッション用の受信ウィンドウ・サイズを L N S に知らせる A V P を追加する。その結果、L N S は、I C R P 応答の適当な受信ウィンドウ・サイズ値だけを含み、ひいては L N S - アンカ L A C - サブ L A C 方向のペイロード・セッションのための 1 つのウィンドウ・サイズだけを含むことになる。）。

【0037】前に述べたように、L N S は接続を承認または拒否する。拒否は結果状態を含まなければならない、エラー表示を含むことがある。どちらの場合でも、L N S は、図 6 に示すように、着信呼応答(Incoming-Call-Reply(ICRP)) メッセージをアンカ L A C に送信する。本発明によれば、次にアンカ L A C は I C R P メッセージを適当に修正し、サブ L A C に中継する（やはり、修正されたフィールドは図 6 では“\*”で示される）。L N S から受信されたパケット処理遅延(P P D) フィールドには L N S の処理遅延だけが含まれるので、アンカ L A C はこの値にそれ自体のノードの処理遅延を追加する。次に、I C R Q メッセージがサブ L A C に中継される。

【0038】それに応答して、サブ L A C は、図 7 に示すように、着信呼接続(Incoming-Call-Connected(ICCN)) メッセージをアンカ L A C に送信する。このメッセージの中で、サブ L A C はすべての L C P 構成要求(Config Request)情報をプロキシ認証情報(Proxy Authentication Information)と共に伝える。すなわち、サブ L A C はユーザの機器で行われた L C P 構成要求/応答(Config Request/Ack)、P P P P A P / C H A P の結果を転送する。アンカ L A C は、受信 I C C N メッセージの P P D フィールドを L N S に中継する前に修正す

る（現在、送信接続速度と受信接続速度は使用されない）。図示されていないが、本発明によれば、アンカ L A C は L 2 T P で定義されたすべての Set-Link-Info、Hello および Wan-Error-Notify メッセージをも中継する

（上記の説明は多重ホップ・パケット・トンネルの概念を示すものであることが観察されるだろう。例えば、図 1 は 2 ホップ・パケット・トンネルを表している）。

【0039】上記で説明した多重ホップ m L 2 T P トンネルはもっぱらフレーム層で発生することが観察されるだろう。すなわち、どんな目的の P P P プロトコル処理でも、遠隔ユーザは L N S と接続するように見えるので、L N S によるアドレス管理の実際の方法は上記で説明した仮想(Virtual)ダイヤルアップ・サービスとは無関係である。

【0040】<移動ポイント・ツー・ポイント・プロトコル>ここで図 8 を参照すると、本発明の概念の他の実施例が示される。図 8 は図 1 と同様である。本発明の概念以外、構成要素は周知であるので、詳細には説明しない。同じ数字は同じ機能を示し、必要な場合以外それ以上説明しない。

【0041】図 8 では、P C 8 0 5 には、パーソナル・コミュニケーション・サービス(P C S)無線ネットワーク 8 1 0 を通じてインターネットへの無線アクセスを確立するデータ通信機器(図示せず)が含まれる。P C S 無線ネットワークは当業技術分野で周知であるので詳細には説明しない。P C S 無線ネットワーク 8 1 0 は、要素 8 1 5 および 8 2 0 で表されるような複数の移動交換センタを備えている。各交換センタはある地理的範囲(図示せず)にサービスを提供する。要素 8 1 5 と 8 2 0 には N A S が含まれることが想定され、例えば、サブ L A C は図 1 のサブ L A C 1 1 5 と同様である。まず、遠隔ユーザが上記で説明した多重ホップ技術を使用して企業のネットワークへの V P N セッションを確立することが想定される。すなわち、遠隔ユーザは、この初期接続が要素 8 1 5 を通じて接続 8 1 4 と 8 1 6 により転送されるような地理的範囲にある。無線 P C S 用の場合、初期 P P P 接続は要素 8 1 5 と P C 8 0 5 の間で行われる（簡単にするために交換要素の一部として示されているが、N A S 機能は機器の独立した部分でも行われる。同様に、ローカル・ネットワークやルータといった他の要素も簡単にするために図示しない。）。

【0042】無線環境では、L 2 T P のようなトンネル・プロトコルによっては遠隔ユーザが既存の P P P 接続を 1 つの交換要素から他の交換要素に変更できないということが認識された。例えば、図 8 が本発明の概念を実施しないことを想定すると、遠隔ユーザが要素 8 2 0（ひいては異なった N A S）のサービスの対象となる地理的範囲に移動する場合、ユーザの通信セッションは、当業技術分野で周知のように要素 8 2 0 に受け渡される。しかし、すでに述べたように、既存の P P P 接続を



1つのNASから別のNASに転送することはできないため、既存のPPP接続（ひいてはVPNセッション）は中断し、復旧しなければならなくなる。この場合、図8の通信システムはこの問題を克服する。

【0043】従って、本発明によれば、NASまたはLACは、既存のNASが既存のPPP接続を別のNASにハンドオフできるようにする「ハンドオフ」機能を組み込んでいる。この機能によれば、(i)継続呼要求(Continued Call Request)、(ii)継続呼応答(Continued Call Reply)および(iii)継続呼接続(Continued Call Connect)という3つの新しい制御メッセージが定義される。上記の結果、ユーザは現行のPPP接続を終了してから新しいPPP接続を復旧する必要はない。この3つの制御メッセージは、L2TP制御メッセージ・ヘッダ、メッセージ識別子（例えば、継続呼要求等）および多数のフィールド（後で説明する）を含んでいる。

【0044】本発明の概念による、ハンドオフ・メッセージの流れの例を図9に示す。図9から観察されるように、トンネル(Tid値で示される)と呼(Cid値で示される)がまず要素815（ここにはサブLACが含まれる）とアンカLACの間に確立される。同様に、アンカLACとLNSの間にトンネルと呼が確立される（この初期VPNセッションを確立する方法は上記で説明済みである）。図9に示すように、本発明の概念によれば、既存のサブLACは既存のPPP接続を、要素820によって表されるような新しいサブLACに転送することができる。

【0045】ここで、「ハンドオフ機能」を提供する際使用される方法の流れ図の例である図10を参照されたい。すでに述べたように、PC805と企業のネットワークの間に要素815を通じたVPNセッションが存在し、そこにサブLACとアンカLAC155が含まれることが想定される。本発明の概念によれば、PCS無線ネットワーク810は既存の呼状態変数に、各無線呼に関するPPP接続の存在（または存在しないこと）を示す追加変数を追加し、PPP接続が存在する場合、例えば、アンカLACのIPアドレスであるアンカLACのIDを含むPPP接続情報を追加する。

【0046】図10のステップ405では、PCS無線ネットワーク810は、PC805が要素815のサービスの対象になる地理的範囲から別の地理的範囲、例えば、要素820のサービスの対象になり、別のサービスLACが含まれる範囲に移動したためハンドオフが必要になったことを検出する。ステップ410では、PCS無線システムは要素820にハンドオフが迫っていることを通知する（ハンドオフを検出し遂行するために無線システムが使用する方法は当業技術分野で周知であり、本発明の概念には関連しない。従って、それらはここでは説明されず、図8の信号経路811で表される）。ここで、呼状態情報にはPPPセッション識別子とPPP

呼情報が含まれているので、（要素820の）新しいサブLACはステップ415でアンカLACを識別する。ステップ420で、（要素820の）新しいサブLACはそれ自体と識別されたアンカLAC（ここではアンカLAC155）の間にすでにトンネルがあるかを確認する。

【0047】トンネルがない場合、新しいサブLACはまずステップ425で（前に説明されたように）トンネルを確立する。次に、本発明の概念によれば、新しいサブLACはステップ430で継続呼要求(Continued-Call-Request(CCRQ))メッセージをアンカLACに送信する。このCCRQメッセージには、既存のPPP接続に関連するユーザ名、移転先の（新しい）PPPセッションで使用されるTidとCidの値が含まれる。

【0048】ステップ435では、アンカLACは受信したCCRQメッセージからユーザ名を回復し、この情報を使用して古いサブLACのLNSとIPアドレスを、例えば、上記の表4で表される接続テーブルから判定する（この回復された情報には対応するユーザ・データグラム・プロトコル(User Datagram Protocol: UDP)ポート番号が含まれることもある）。このステップでは、アンカLACは呼切断通知(Call-Disconnect-Notify)メッセージ（例えば、L2TP参照）を古いサブLACに送信し、かつ、例えば、上記の表4で、古いトンネルidや古い呼idといった遠隔ユーザへのこのPPP接続に関連する既存の呼変数を識別する（他方、アンカLACが継続呼要求(Continued-Call-Request)を拒否した場合、サブLACは、既存のPPPセッションが切断され、新しいPPPセッションが開始されるか、または単にPPPセッションが中止されるように信号を返送する（このステップは図示しない））。

【0049】ステップ440では、アンカLACが適当な受信ウィンドウ・サイズで継続呼応答(Continued-Call-Reply: CCRP)メッセージによって応答する。CCRPメッセージには現行のNrとNsの値に関する情報が含まれる。ステップ445では、（ステップ435で識別された）Tid、CidおよびサブLACのIPアドレス・フィールドのエントリを既存のPPP接続の新しい呼情報に置換することにより、接続テーブル（例えば、上記の表4）を更新する。ステップ450では、新しいサブLACはNr、NsをSr、Ss値に保存し、かつ必要な場合受信したCCRPメッセージから受信ウィンドウ・サイズを保存し、継続呼接続(Continued-Call-Connect: CCCN)メッセージをアンカLACに送信し、これをもってハンドオフを完了する。

【0050】PPPプロトコルの上記で説明したハンドオフ機能を裏付けるものとして、図11は本発明の原理による上記で言及した新しい制御メッセージ・トランザクションの例を示す。図11に示すように、CCRQメッセージが識別されたアンカLACに送信される。



【0051】CCRQメッセージは次のフィールドを含む。

- ー割当てC i d
- ー呼シリアルナンバー
- ーベアラ(bearer)の種類
- ー物理チャネルID
- ーダイヤルされた番号
- ーダイヤルする番号
- ー副アドレス
- ーアンカLAC
- ーチャレンジ
- ーユーザAVP
- ーユーザ名
- ーユーザのMIN/電話番号

【0052】アンカLACのフィールドは、この情報がハンドオフの際に利用可能であることを想定している

(また、ハンドオフ処理がアンカLACに関する情報を新しいサブLACに提供しない場合、ハンドオフ処理は、当業技術分野で周知のように新しいサブLACが外部ラディアスサーバの助けによってアンカLAC情報を検索する十分なユーザ情報を新しいサブLACに提供しなければならない。すなわち、新しいサブLACはラディアスアクセス/応答メッセージにより、ホームラディアスサーバからアンカLACについて照会する)。

【0053】ユーザAVP情報には(ユーザ名のよう)なユーザ情報と、例えば、多重ホップ仮想ダイヤルアップ・サービス、ユーザのID(MIN)、サービス・プロバイダの電話番号等といった他のユーザの信用証明が含まれる。

【0054】CCRQメッセージに続いて、アンカLACは呼切断通知(Call-Disconnect-Notify)メッセージを古いサブLACに送信する。次に、アンカLACは、保守の対象となる現行Sr、Ssを含む継続呼応答(Continued-Call-Reply:CCRP)メッセージによって応答する。

【0055】CCRPメッセージは次のフィールドを含む。

- ー割当てC i d
- ー結果コード
- ー受信ウィンドウ・サイズ
- ーPPD
- ーNr
- ーNs
- ーチャレンジ
- ーチャレンジ応答

【0056】最後に、新しいサブLACが継続呼接続(Continued-Call Connect:CCCN)によって応答する。CCCNメッセージは次のフィールドを含む。

- ー接続速度

ーフレーム種類

ー受信ウィンドウ・サイズ

ーPPD

ーチャレンジ応答

【0057】ここで図12を参照すると、既存のPPP接続を1つのNASから別のNASに移転し、その際古いNASがLNSに接続している場合、本発明の概念の他の実施例が示される(この例では、サブLACは本質的に存在せず、例えば、もっと簡単に、アンカLACが既存のPPP接続を直接サポートする)。図12は図8と同様である。本発明の概念以外、構成要素は周知であるので、詳細には説明しない。同じ数字は同じ機能を示し、必要な場合以外それ以上説明しない。

【0058】図12では、PC805には、パーソナル・コミュニケーション・サービス(Personal Communication Service:PCS)無線ネットワーク910を通じてインターネットへの無線アクセスを確立するデータ通信機器(図示せず)が含まれる。PCS無線サービスは当業技術分野で周知であるので詳細には説明しない。PCS無線ネットワーク910は要素875および880で表されるような複数の移動交換センタを含む。各交換センタはある地理的範囲(図示せず)にサービスを提供する。要素875と880には、例えば、図1のアンカLAC115と同様のLACであるNASが含まれる。まず、遠隔ユーザが、例えば、L2TPの該当部分を使用して、当業技術分野で周知のように企業のネットワークへのVPNセッションを確立することが想定される。すなわち、遠隔ユーザはこの最初の接続が要素875を通じて接続874と876によりLNS935に転送されるような地理的範囲にある。無線PCS適用業務の場合、初期PPP接続は要素875とPC805の間で行われる(簡単にするために交換要素の一部として示されているが、NAS機能は機器の独立した部分でも行われる。同様に、ローカル・ネットワークやルータといった他の要素も簡単にするために図示しない)。

【0059】この実施例では、上記で説明したCCRQ、CCRP、CCCNメッセージが新しいLACとLNSの間で交換される点以外は、同じハンドオフ手順がLAC/LNSペアについて実行される。本発明の概念による、ハンドオフ・メッセージの流れの例を図13に示す。図13から観察されるように、トンネル(Tid値で示される)と呼(Cid値で示される)がまず要素875(ここにはLACが含まれる)とLNS935の間に確立される。図13に示すように、本発明の概念は、既存のLACが既存のPPP接続を、要素880で表される新しいLACに移転することを可能にする。

【0060】ここで、「ハンドオフ機能」を提供する再使用される方法の流れ図の例である図14を参照されたい。すでに述べたように、PC805と企業のネットワークの間に、LACを含む要素875を通じてVPNセ

セッションが存在していることが想定される。本発明の概念によれば、PCS無線ネットワーク910は既存の呼状態変数に、各無線呼に関するPPP接続の存在（または存在しないこと）を示す状態変数を追加し、PPP接続が存在する場合、例えば、LNSのIPアドレスであるLNSのIDを含むPPP接続情報を追加する。

【0061】図14のステップ505では、PCS無線ネットワーク910は、PC805が要素875のサービスの対象になる地理的範囲から別の地理的範囲、例えば、要素880のサービスの対象になり、別のサービスLACが含まれる範囲に移動したためハンドオフが必要になったことを検出する。ステップ510では、PCS無線システムは要素880にハンドオフが迫っていることを通知する（ハンドオフを検出し遂行するために無線システムが使用する方法は当業技術分野で周知であり、本発明の概念には関連しない。従って、それらはここでは説明されず、図12の信号経路911で表される）。ここで、呼状態情報にはPPPセッション識別子とPPP呼情報が含まれているので、（要素880の）新しいLACはステップ515でアンカLACを識別する。ステップ520で、（要素880の）新しいLACはそれ自体と識別されたLNS（ここではLNS935）の間にすでにトンネルがあるかを確認する。

【0062】トンネルがない場合、新しいLACはまずステップ525で（前に説明されたように）トンネルを確立する。次に、本発明の概念によれば、新しいLACはステップ530で継続呼要求(Continued-Call-Request: CCRQ)メッセージをLNSに送信する。このCCRQメッセージには、既存のPPP接続に関連するユーザ名、移動先の（新しい）PPPセッションで使用されるTidとCidの値が含まれる。

【0063】ステップ535では、LNSは受信したCCRQメッセージからユーザ名を回復し、この情報を使用して古いLACのIPアドレスを判定する（この回復された情報には対応するユーザ・データグラム・プロトコル(UDP)ポート番号が含まれることもある）。このステップでは、アンカLACは呼切断通知(Call-Disconnect-Notify)メッセージ（例えば、L2TP参照）を古いLACに送信し、かつ、例えば、上記の表4で示されるものと同様だが、サブLAC情報等は除く接続テーブルで、古いトンネルidや古い呼idといった遠隔ユーザへのこのPPP接続に関連する既存の呼変数を識別する（他方、LNSが継続呼要求(Continued-Call-Re

quest)を拒否した場合、新しいLACは、既存のPPPセッションが切断され、新しいPPPセッションが開始されるか、または単に古いPPPセッションが中止されるように信号を返送する（このステップは図示しない）。

【0064】ステップ540では、LNSが適当な受信ウィンドウ・サイズで継続呼応答(Continued-Call-Reply: CCRP)メッセージによって応答する。CCRPメッセージには現行のNrとNsの値に関する情報が含まれる。ステップ545では、LNSは、（ステップ535で識別された）Tid、CidおよびLACのIPアドレス・フィールドのエントリを既存のPPP接続の新しい呼情報に置換することにより、接続テーブルを更新する。ステップ550では、新しいLACはNr、Nsを更新し、必要な場合受信したCCRPメッセージからNr、Nsと受信ウィンドウ・サイズを更新し、継続呼接続(Continued-Call-Connect: CCCN)メッセージをLNSに送信し、これをもってハンドオフを完了する。

【0065】PPPプロトコルの上記で説明したハンドオフ機能を裏付けるものとして、図15は本発明の原理による新しい制御メッセージ・トランザクションを示す。図15に示すように、CCRQメッセージが識別されたLNSに送信される（また、ハンドオフ処理がLNSに関する情報を新しいLACに提供しない場合、ハンドオフ処理は、当業技術分野で周知のように新しいLACが外部ラディアスサーバの助けによってLNS情報を検索する十分なユーザ情報を新しいLACに提供しなければならない。すなわち、新しいLACはラディアスアクセス/応答メッセージにより、ホームラディアスサーバからLNSについて照会する）。CCRQメッセージに続いて、LNSは呼切断通知(Call-Disconnect-Notify)メッセージを古いLACに送信する。次に、LNSは、保守の対象となる現行Sr、Ssを含む継続呼応答(Continued-Call-Reply: CCRP)メッセージによって応答する。最後に、新しいLACが継続呼接続(Continued-Call-Connect: CCCN)によって応答する。

【0066】上記で説明したように、PPP接続は1つのNASから別のNASに移転される。新しく定義されたメッセージを裏付けるものとして、以下図5および図6に示されるように対応するNASについて追加呼状態が定義される。

【表5】

呼状態	イベント	動作	新しい状態
アイドル	ハンドオフ通知	CCRQを送信する	CCRP応答待ち
CCRP応答待ち	CCRPを受信する、 承認されない	クリーンアップ	アイドル
CCRP応答待ち	CCRP受信する、 承認	CCCNを送信する	確立

表5-新しいLAC(またはNAS)

【0067】観察されるように、継続される呼について新しいLAC(またはNAS)に関連するmL2TPの追加された、または新しい呼状態はCCRP応答待ち状態である。

【0068】古いLAC(またはNAS)について、確

立された状態で呼切断通知(Call-Disconnect-Notify:CDN)メッセージが受信されることに留意されたい。それに応答して、古いLACは呼をクリーンアップして切断し、アイドル状態に戻る。

【表6】

呼状態	イベント	動作	新しい状態
確立	CCRQを受信した 承認されない	エラーコードと共に CCRPを送信する CDNをLNSに送信する	アイドル
確立	CCRPを受信する 承認	CDNを古いLACに送信する CCRPを新しいLACに送信する	CCCN待ち
CCCN待ち	CCCNを受信する	データの準備完了	確立
CCCN待ち	CCCNを受信する	クリーンアップ	アイドル

表6-アンカーLACまたはLNS

【0069】観察されるように、継続される呼について、アンカーLACまたはLNSに関連するmL2TPの追加された、または新しい呼状態はCCCN待ち状態である。

【0070】<ペイロード・メッセージの概観とmL2TPの輻輳制御>mL2TPのペイロード・メッセージに関して、サブLACとLNSはL2TP手順を遵守する。アンカーLACはペイロード・パケットについてTidとCidをスワップする。また、アンカーLACはサブLACが送信する(Nr、Ns)値を監視する(サブLACとアンカーLACの間にはパケット損失が存在するので、アンカーLACのSrおよびSsの値はどちらもサブLACが保守するこれらの数値より遅れると考えられることに留意されたい。)アンカーLACはどちらの方向でもペイロード・パケットの(Nr、Ns)を変更しない。アンカーLACは、継続呼要求(Continued-Call-Request)メッセージを新しいサブLACから受信する時それ自体のSr、Ss値だけを利用する。

【0071】輻輳制御に関して、L2TPは受信ウィンドウ・サイズを維持する時期、Nr/Nsを送信する時期およびACKを送信する時期に関するL2TPの要求をmL2TPに適用する。さらに、mL2TPはサブLACとアンカーLACについて次の追加要求を有する。

【0072】アンカーLACはサブLACが送信した(Nr、Ns)値の監視が必要である。アンカーLAC

は、サブLACから受信する継続呼接続(Continued-Call-Connect)メッセージに応答する時継続呼応答(Continued-Call-Reply)メッセージの中で保守する(Sr、Ss)値を含むべきである。サブLACとアンカーLACの間のネットワークは損失が大きいので、アンカーLACが保守するSr値はサブLACより遅れることがある。

【0073】さらに、サブLACは、当業技術分野の用語に従えば、単純なレシーバではなく完全なレシーバである。この要求は、PPPセッションの継続期間中にサブLACの変更がある場合、新しいサブLACがシーケンス外や重複したパケットを上部層に伝えないということである。

【0074】簡単に図16を参照すると、代表的なNASの高レベル・ブロック図が示される。NASは蓄積プログラム制御ベース・プロセッサ・アーキテクチャであり、プロセッサ650、メモリ660(プログラムの命令と、上記で言及した接続テーブル等のデータを保存する)および経路666で表されるように1つかそれ以上の通信機能を結合する通信インタフェース665を含む。

【0075】以上は本発明の原理を例示したものに過ぎず、当業技術分野に熟練した者には、ここで明示的に説明されていなくとも、本発明の原理を実施しその精神と範囲の中にある非常に多くの代替装置が考案できること

を認識することができるだろう。例えば、本発明の概念はサブNASが着信呼に関する多重ホップ・トンネルの確立を開始する場合で説明されたが、本発明の概念は、例えば、LNSが発信呼に関する多重ホップ・シーケンスを開始する場合にも等しく適用できる。こうした修正は簡単明瞭であり、図17及び図18で示されているのでここでは説明しない。

【図面の簡単な説明】

【図1】本発明の原理による通信システムを示す図である。

【図2】図1の通信システムを使用する例示としての方法の流れ図を示す図である。

【図3】図1の通信システムを使用する例示としての方法の流れ図を示す図である。

【図4】例示としての多重ホップ・メッセージの流れを示す図である。

【図5】例示としての制御メッセージのトランザクションを示す図である。

【図6】例示としての制御メッセージのトランザクションを示す図である。

【図7】例示としての制御メッセージのトランザクションを示す図である。

【図8】本発明の原理による通信システムの他の実施例を示す図である。

【図9】例示としてのハンドオフ・メッセージの流れを示す図である。

【図10】図8の通信システムで使用される例示としての方法の流れ図を示す図である。

【図11】例示としての制御メッセージのトランザクションを示す図である。

【図12】本発明の原理による通信システムの他の実施例を示す図である。

【図13】例示としてのハンドオフ・メッセージの流れを示す図である。

【図14】図12の通信システムで使用される例示としての方法の流れ図を示す図である。

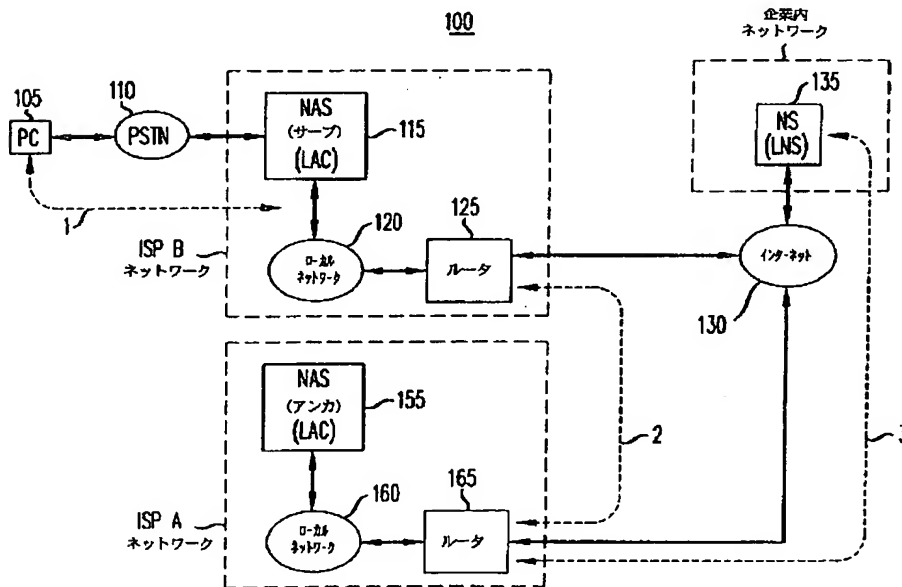
【図15】例示としての制御メッセージのトランザクションを示す図である。

【図16】ネットワーク・アクセス・サーバの例示としての高レベル・ブロック図を示す図である。

【図17】発信呼用の例示としての制御メッセージ・トランザクションを示す図である。

【図18】発信呼用の例示としての制御メッセージ・トランザクションを示す図である。

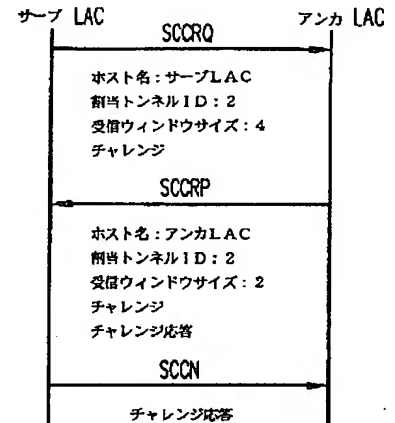
【図1】



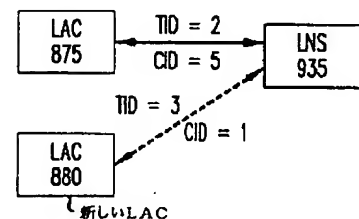
【図4】



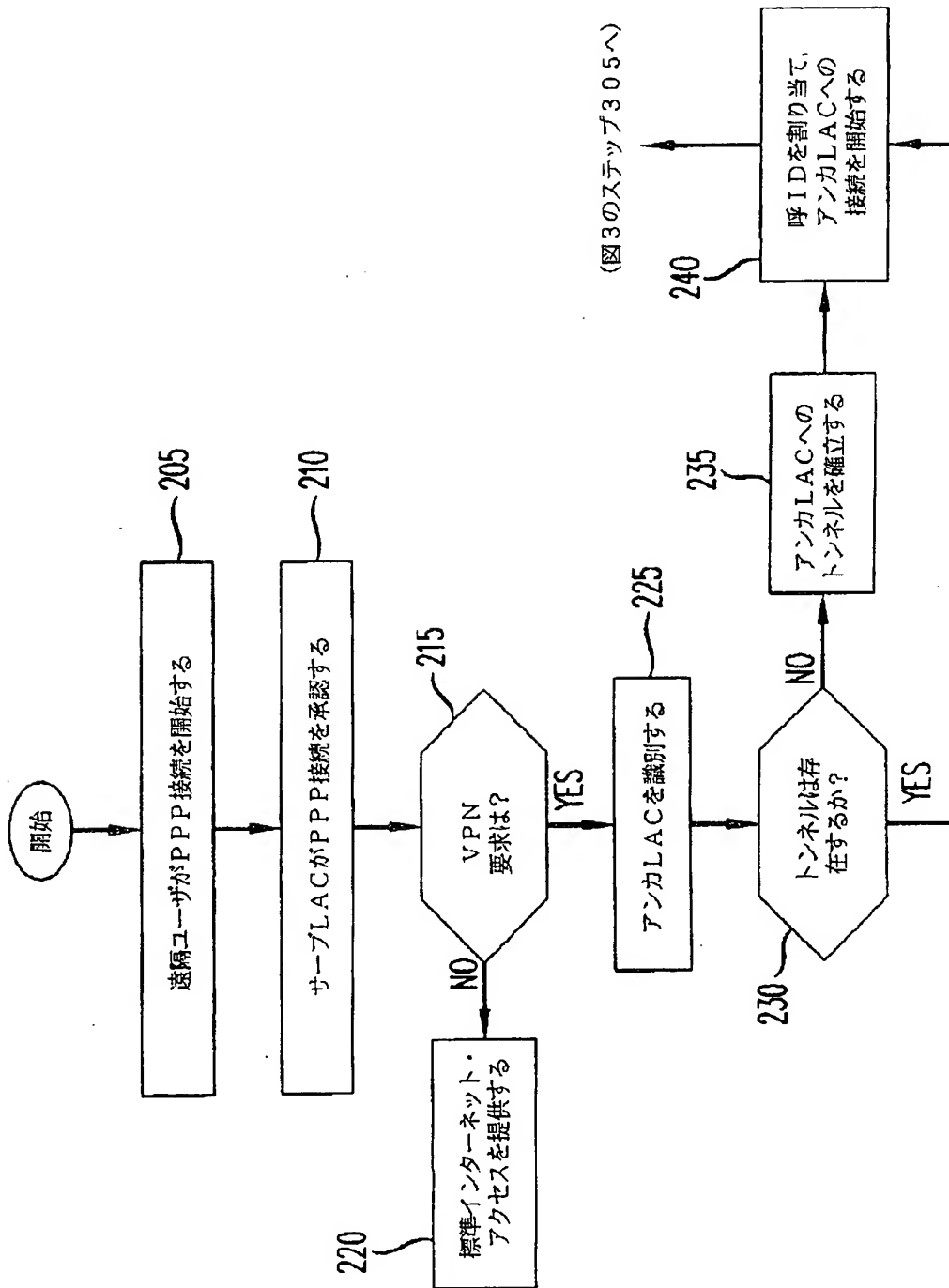
【図5】



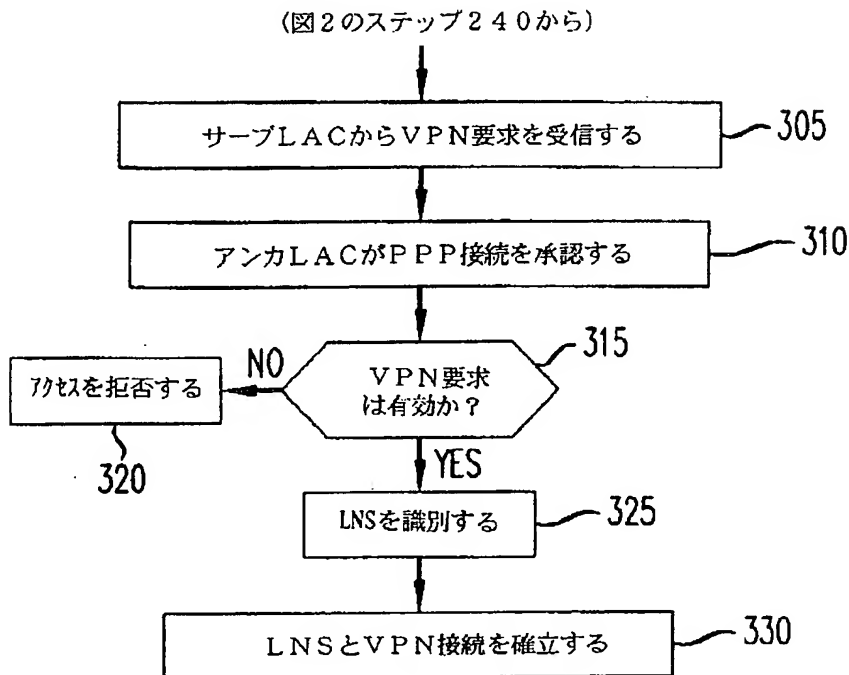
【図13】



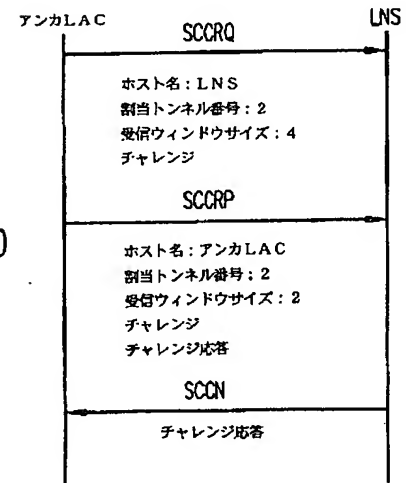
【図 2】



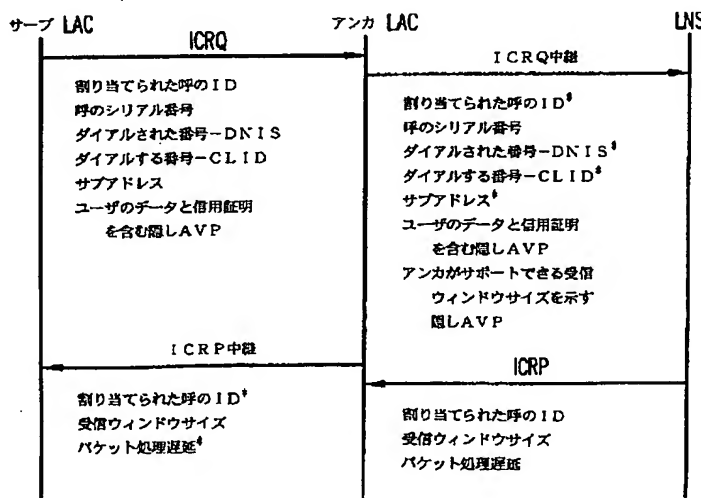
【図3】



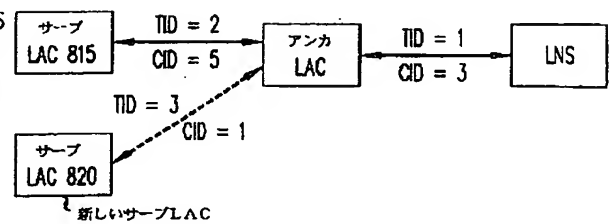
【図17】



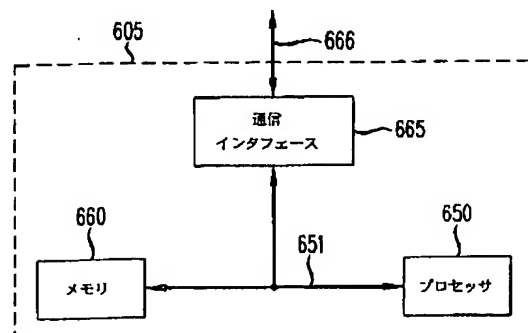
【図6】



【図9】

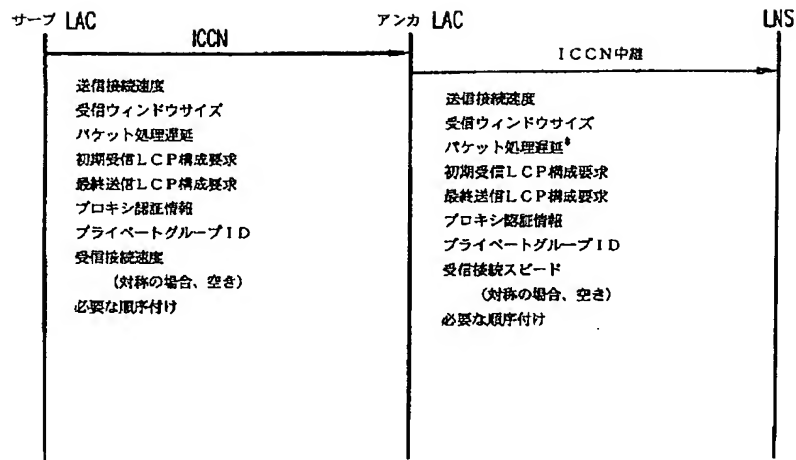


【図16】

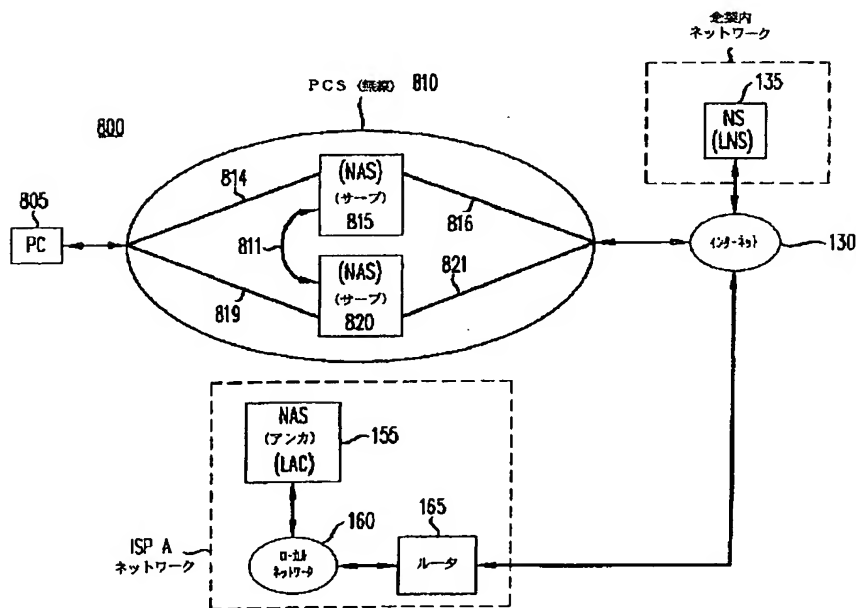




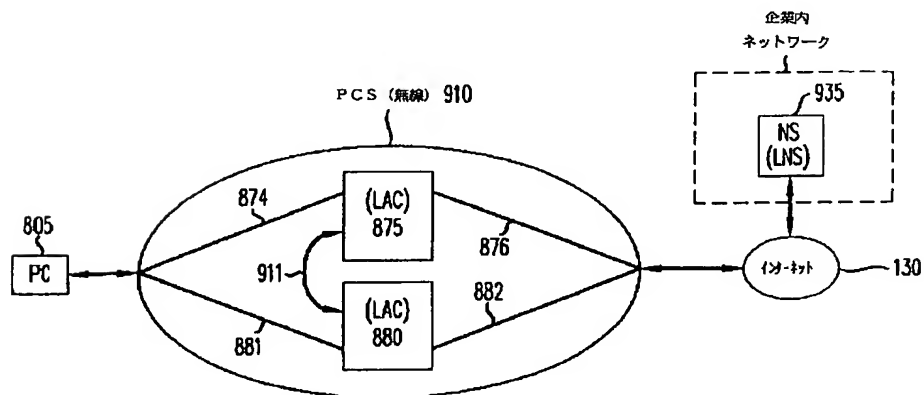
【図 7】



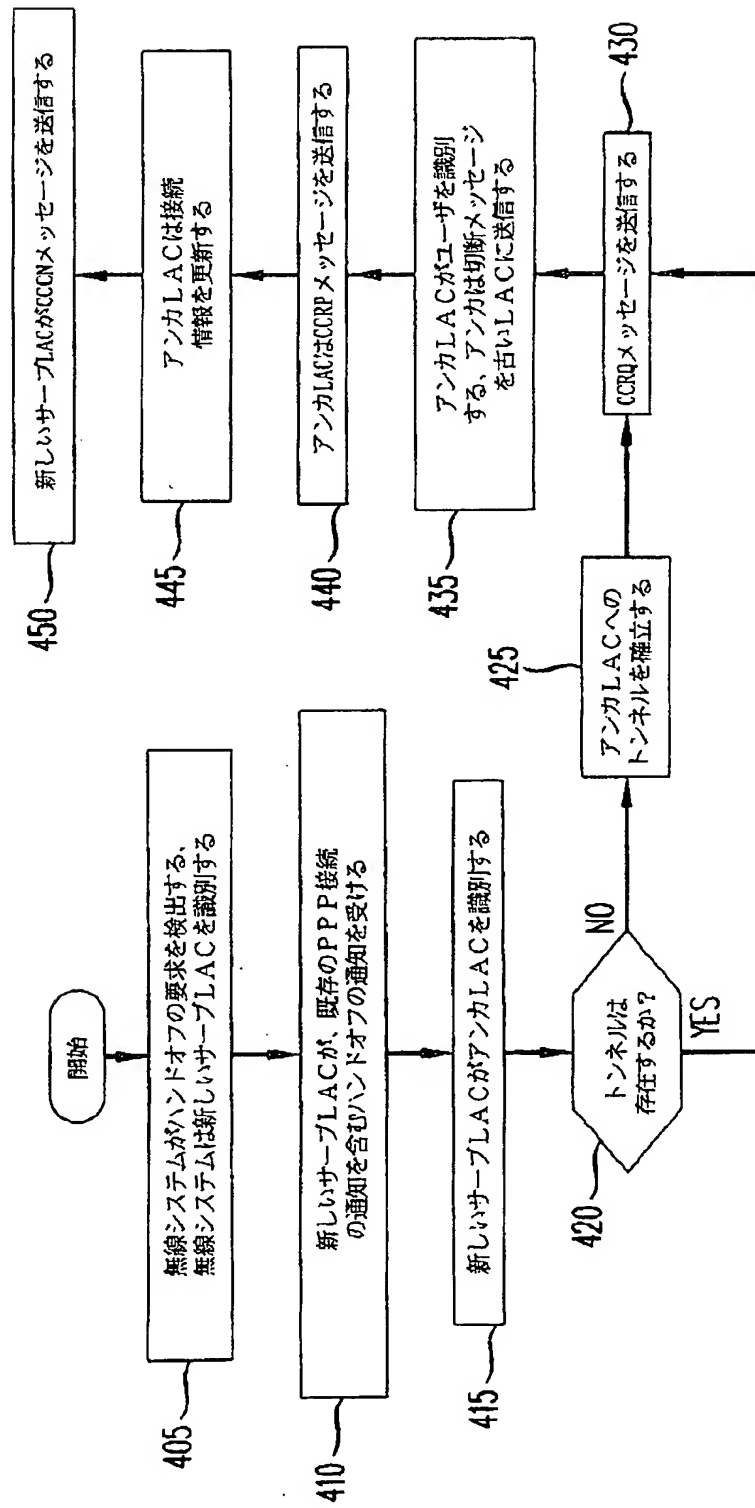
【図 8】



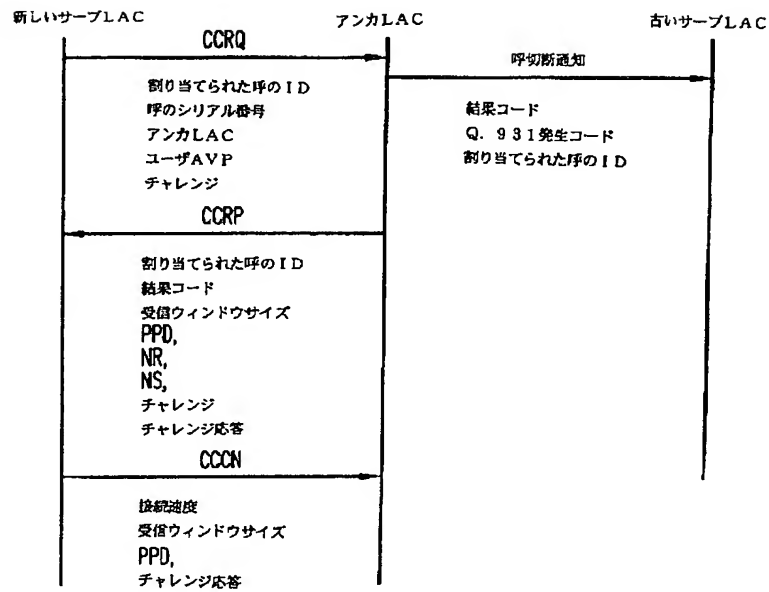
【図 12】



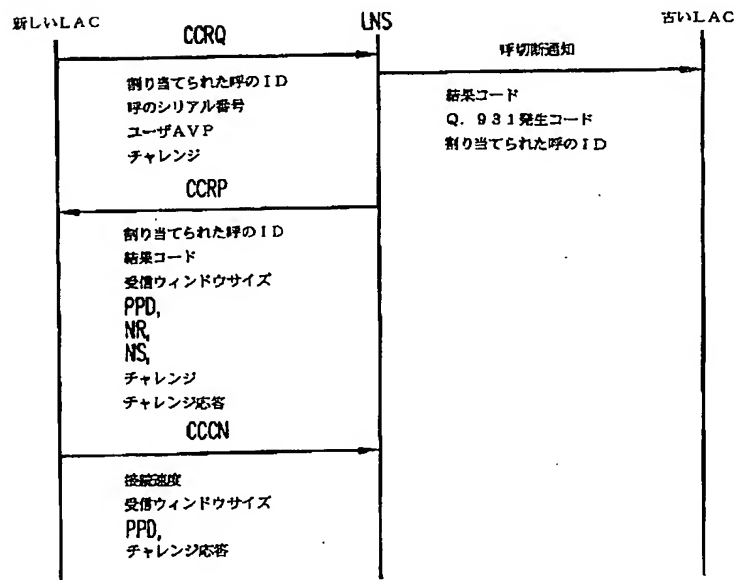
【図 10】



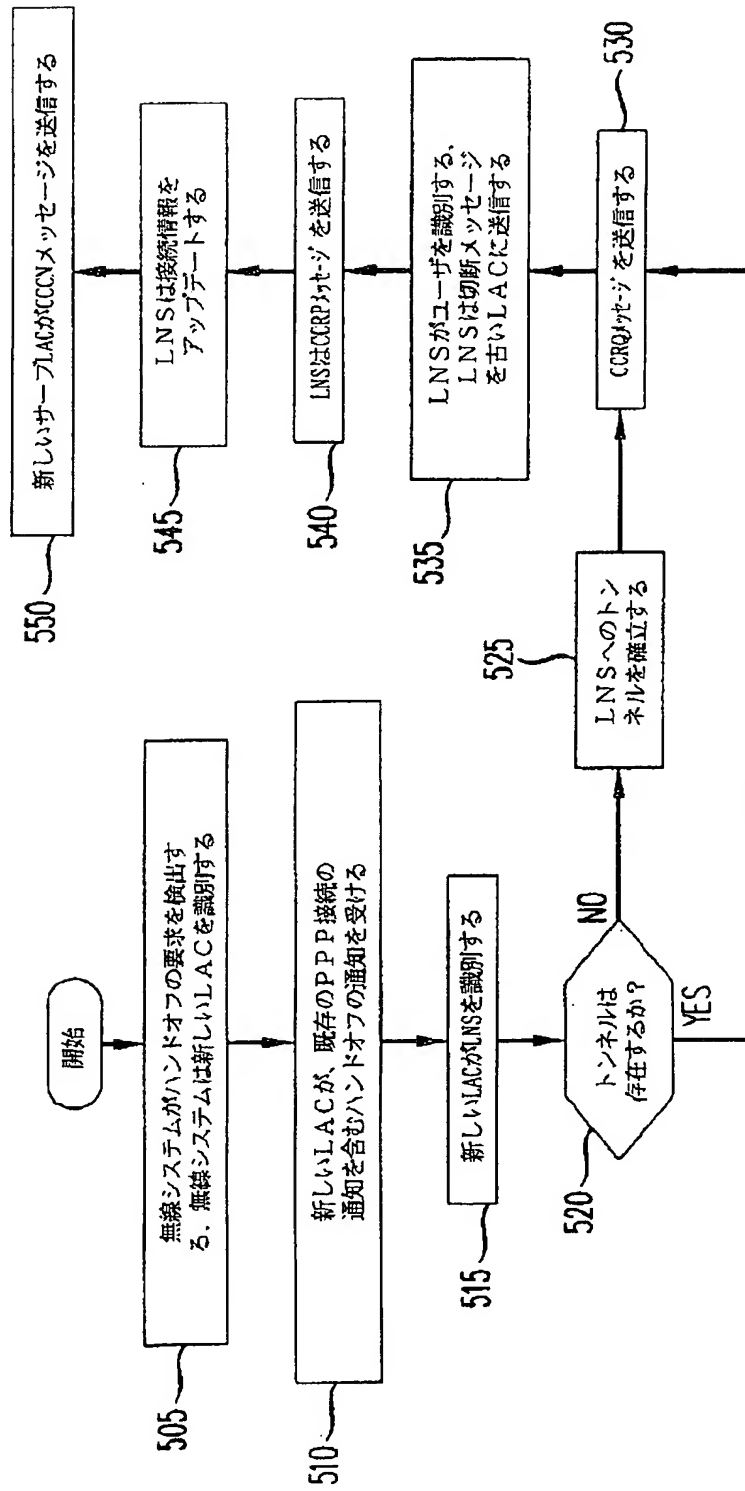
【図 11】



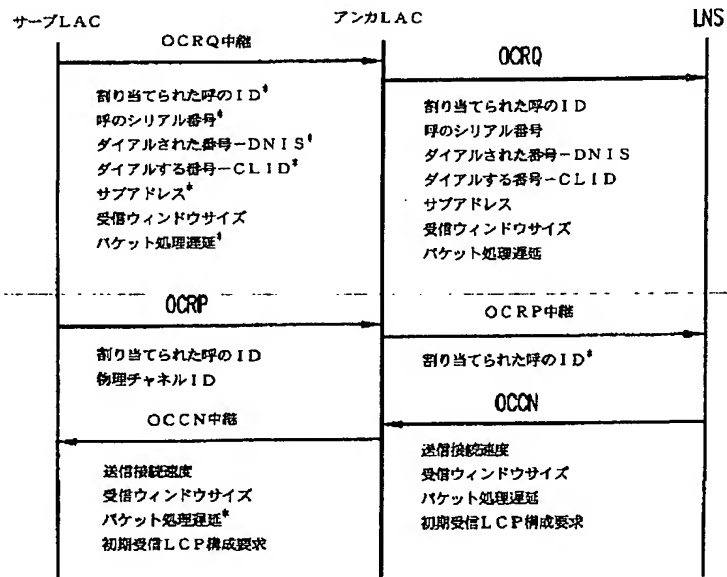
【図 15】



【図 1 4】



【図 1 8】



フロントページの続き

(72)発明者    ギリッシュ・ライ  
                アメリカ合衆国 60103    イリノイズ, バ  
                ートレット, レディ スミス    ロード  
523

【公報種別】特許法第 17 条の 2 の規定による補正の掲載

【部門区分】第 7 部門第 3 区分

【発行日】平成 13 年 7 月 27 日 (2001. 7. 27)

【公開番号】特開平 11-355272

【公開日】平成 11 年 12 月 24 日 (1999. 12. 24)

【年通号数】公開特許公報 11-3553

【出願番号】特願平 11-126563

【国際特許分類第 7 版】

H04L 12/22

12/56

【F I】

H04L 11/26

11/20 102 A

【手続補正書】

【提出日】平成 12 年 8 月 18 日 (2000. 8. 18)

【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項 1】 パケット・サーバで使用される方法であって、該方法が、多重ホップ・パケット・トンネルを他のパケット終端間に確立する段階と、  
該多重ホップ・パケット・トンネルを通じて該他のパケット終端間でメッセージを中継する段階とからなることを特徴とする方法。

【請求項 2】 請求項 1 に記載の方法において、該確立する段階が、  
1 つのパケット終端への第 1 のパケット・トンネルを確立する段階と、  
別のパケット終端への第 2 のパケット・トンネルを確立する段階とからなることを特徴とする方法。

【請求項 3】 請求項 2 に記載の方法において、該方法はさらに、接続情報を追跡する段階からなり、該接続情報は、該第 1 のパケット・トンネルに関するトンネル識別値と該第 2 のパケット・トンネルに関するトンネル識別値とを含むことを特徴とする方法。

【請求項 4】 請求項 1 に記載の方法において、該中継段階は、該他のパケット終端間で中継する前に、該メッセージの少なくとも一部を修正する段階を含むことを特徴とする方法。

【請求項 5】 請求項 1 に記載の方法において、該中継段階は、該他のパケット終端間で中継する前に、該メッセージの少なくとも一部のトンネル識別情報を修正する段階を含むことを特徴とする方法。

【請求項 6】 請求項 1 に記載の方法において、該中継段階は、該他のパケット終端間でメッセージを中継する前に、何れかのメッセージに含まれるパケット処理遅延情報を修正して、該パケット・サーバに関するパケット処理遅延を含ませる段階を含むことを特徴とする方法。

【請求項 7】 請求項 1 に記載の方法において、該パケット・サーバが多重トンネルをサポートするインターネット・プロトコルを使用することを特徴とする方法。

【請求項 8】 請求項 7 に記載の方法において、該インターネット・プロトコルがレイヤ 2 トンネル・プロトコルの形態であることを特徴とする方法。

【請求項 9】 パケット・ネットワークで使用される装置であって、該装置はパケット・サーバからなり、該パケットサーバは、

a) 仮想私設網サービスにアクセスするためにユーザとのポイント・ツー・ポイント・プロトコル接続を承認し、そして b) ホップ間に配置されホップ間でメッセージを中継するように、他のパケット・サーバとの多重ホップ・トンネル接続を承認することを特徴とする装置。

【請求項 10】 請求項 9 に記載の装置において、該パケット・サーバは、該メッセージの少なくとも一部をホップ間で中継する前に修正することを特徴とする装置。

【請求項 11】 請求項 9 に記載の装置において、該パケット・サーバは、該メッセージの少なくとも一部のトンネル識別情報をホップ間で中継する前に修正することを特徴とする装置。

【請求項 12】 請求項 9 に記載の装置において、該パケット・サーバは、ホップ間でメッセージを中継する前に、何れかの該メッセージに含まれるパケット処理遅延情報を修正して、該パケット・サーバに関するパケット処理遅延を含むことを特徴とする装置。

【請求項 13】 請求項 9 に記載の装置において、該パケット・サーバは、多重トンネルをサポートするインターネット・プロトコルを使用することを特徴とする装



置。

【請求項 1 4】 請求項 1 3 に記載の装置において、該 インターネット・プロトコルがレイヤ 2 トンネル・プロトコルの形態であることを特徴とする装置。